ifm electronic

Safety and availability of machinery.

Safety Integrity Level SIL
Performance Level PL

Safety Technology

www.ifm.com/gb/safe

fluid sensors and diagnostic systems

position sensors and object recognition

bus, identification and control systems

ifm electronic – close to you!

For industrial applications

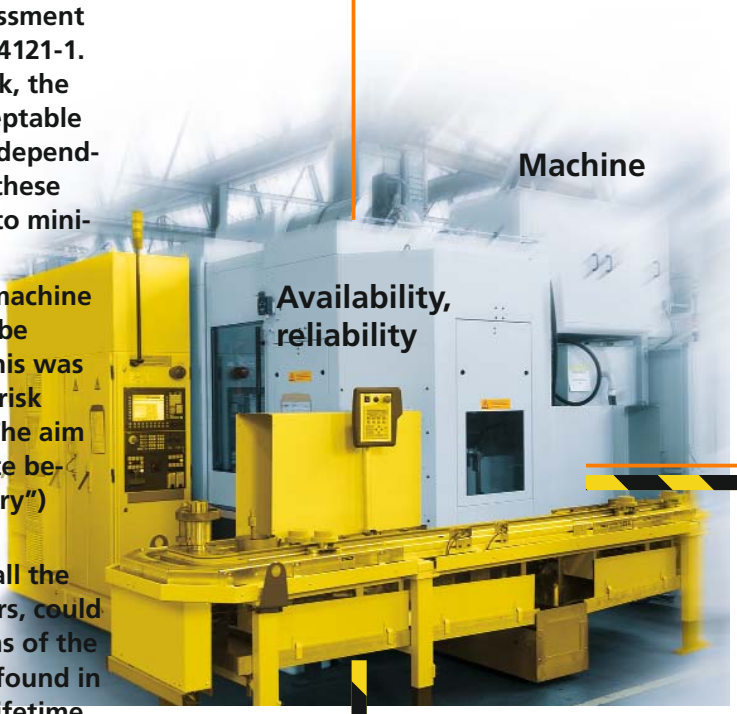
The EC Machinery Directive stipulates machinery should not present a risk – risk assessment to EN 1050 and EN ISO 14121-1. Since there is no zero risk, the aim is to achieve an acceptable residual risk. If safety is dependent on control systems, these must be designed so as to minimise malfunction.

Safety-related parts of machine control systems used to be designed to EN 954-1. This was based on the calculated risk (formed in categories). The aim was to set an appropriate behaviour ("control category") against a category.

New electronics, above all the programmable controllers, could not be measured in terms of the simple category system found in EN 954-1. Test interval, lifetime and probability of failure were, for example, not considered in the old standard.

Help is now available from EN 62061 and EN ISO 13849-1, the successor standard of EN 954-1.

The classification is made either in the Safety Integrity Level (SIL 1-3 in EN 62061) or in the Performance Level (PL a-e in EN ISO 13849-1).



Assessing availability and reliability

Analysing risk

Step by step to safety –
Step 1
Risk assessment to EN 1050 / EN ISO 14121-1

Without any protective measures a risk will lead to harm. Therefore the designer has to assess the risk as below:

- establish the limits and the intended use of the machinery
- identify any hazardous situations
- assess the risk for each hazard identified
- estimate the risk and decide on the need for risk reduction

Terms and abbreviations reliability / availability

***MTBF** Mean Time Between Failures*
The average (statistical) time (expectation) between two failures

***MTTF** Mean Time To Failures*
The average (statistical) time (expectation) to failure

***MTTR** Mean Time To Repair*
The average repair time (always considerably smaller than MTTF)

Availability (A)
The availability is the probability to find a repairable item at a defined point of time t in the "functional" state

Reliability (function) R(t)
The reliability function R(t) (survival probability) is the probability that an item is functional in an assessment period (0...t)

Probability of failure F(t)
The probability of failure F(t) is the complement of the reliability function R(t)

Terms and abbreviations functional safety

SRECS
Safety-related electrical / electronic control system

SRP / CS
Safety-related part of a control system

CCF
Common cause failure

DCavg
Average diagnostic coverage (relationship between the failure rate of the noticed dangerous failures and the failure rate of the total dangerous failures)

***MTTFd** Mean time to dangerous failure*
Average (statistical) time (expectation) to dangerous failure (EN ISO 13849)

PFH / PFHd
Average probability of a dangerous failure per hour (corresponds to a [failure] rate of dangerous failures) (IEC 61508 / EN 62061)

SFF
Safe failure fraction (IEC 61508 / EN 62061)

PL
Ability of safety-related parts to perform a safety function under foreseeable conditions to achieve the expected risk reduction (EN ISO 13849)

PL_r
Required performance level for each safety function SF (e.g. from risk graph)

SIL
Safety integrity level

SIL_{CL}
SIL claim limit (suitability) (e.g. for a subsystem -> sensor)

***T1** (Test interval)*
Interval of the repetition test or mission time (in hours) (IEC 61508/ EN 62061)

***T_M** (mission time)*
Mission time (EN ISO 13849-1)

Risk
The product of probability of occurrence of the damage and the extent of damage

Risk reduction
Reduction of the hazard by using systems or organisation methods

Residual risk
The residual risk is the hazard remaining even after all safety measures theoretically possible have been taken.

B10d
The B10d value for components subject to wear is expressed in the number of cycles: This is the number of cycles during which 10 % of the specimen failed dangerously in the course of a lifetime test.

Frequently asked questions

1. Is there an analogy between PL and SIL?

A relationship between PL and SIL can be established through the PFH value.

PL Performance Level (EN ISO 13849-1)	Average probability of a dangerous failure per hour	SIL to EN 62061
a	$10^{-5} \leq PFH < 10^{-4}$	–
b	$3 \cdot 10^{-6} \leq PFH < 10^{-5}$	SIL1
c	$10^{-6} \leq PFH < 3 \cdot 10^{-6}$	SIL1
d	$10^{-7} \leq PFH < 10^{-6}$	SIL2
e	$10^{-8} \leq PFH < 10^{-7}$	SIL3

PFH: Probability of failure per hour (average probability of a dangerous failure per hour)

2. Does the MTTF indicate the guaranteed lifetime?
No. The MTTF is a mathematical average value of the time to failure. For electronic systems ≈ 63 % failed from the statistical point of view after the time t = MTTF.

3. Is there a PFH value for components that are subject to wear?
The user can calculate a PFH value for wearing components using the B10d value in relation to the number of duty cycles.

4. Does application software have to be certified? If yes, to what standard?
No. There is no mandatory certification / approval for either standard. There may, however, be mandatory certification/approval for Annex IV-machines. Requirements for software production can be found in both EN 62061 and EN ISO 13849-1.

5. What does the letter "d" mean on MTTFd?
"d" stands for "dangerous", the MTTFd describes the mean (statistical) time to a dangerous failure.

6. What difference is there between reliability and safety?
***Reliability:** Total of characteristics referring to the suitability for fulfilling the requirements at given conditions for a given time interval.*
***Safety:** Circumstances under which the risk is not greater than the limit risk, include the ability not to cause or not to let occur any risk for a given period of time within defined limits.*

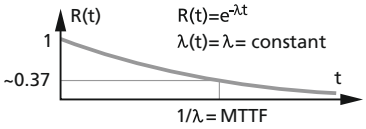
7. Are safety modules required for the operation of machinery / plant?
No. Standard components may be used for the operation of machinery / plant.

ifm electronic provides characteristic values (MTTF, MTBF) for the calculation of reliability / availability of electronic systems:

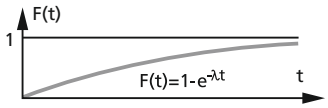
MTBF;
MTTF;
MTTR;
Availability (A)

$$A = \frac{MTTF}{MTBF}$$

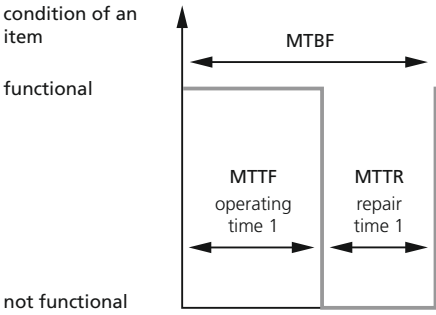
Reliability (function) R(t)



Probability of failure F(t)



Operating and maintenance units



Step 2
Defining the measures required to reduce the calculated risks

The objective is to reduce risk as much as possible, taking various factors into account.

- safety of the machine in all phases of its mission time
- ability of the machine to perform its function
- user friendliness of the machine

Only then shall the machines manufacturing, operating and disassembly costs be taken into consideration.

The hazard analysis and the risk reduction process require hazards to be eliminated or reduced through a hierarchy of measures:

- hazard elimination or risk reduction through design
- risk reduction through protection devices and additional protective measures
- risk reduction through the availability of user information about residual risk

Step 3
Risk reduction through control measures

If the risk is to be reduced by taking control measures, the design of safety-relevant control units is an integral part of the whole design procedure for the machine.

The safety-relevant control system will provide the safety function(s) with a SIL or PL which achieves the necessary risk reduction.

Step 4
Implementation of control measures using

EN 62061:

This standard is to be applied to safety-related electrical, electronic and programmable control systems for machines.

EN ISO 13849-1:

This standard may be applied to safety-related parts of control systems and all types of machinery regardless of the type of technology and energy used (electrical, pneumatic, hydraulic, mechanical, etc).

Requirement of the requested SIL

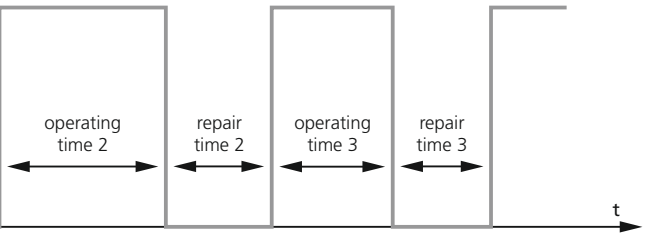
Determination of the required PL_r

EN 62061

Consequences	Extent of injury S
Death, losing an eye or arm	4
Permanent, losing fingers	3
Reversible, medical attention	2
Reversible, first aid	1

Severity of injury S	
slight (normally reversible) injury	S1
serious (normally irreversible) injury	S2
Frequency and / or exposure to a hazard F	
seldom to less often and / or the exposure time is short	F1
frequent to continuous and / or the exposure time is long	F2
Possibility of avoiding the hazard or limiting the harm P	
possible under specific circumstances	P1
scarcely possible	P2

of an item

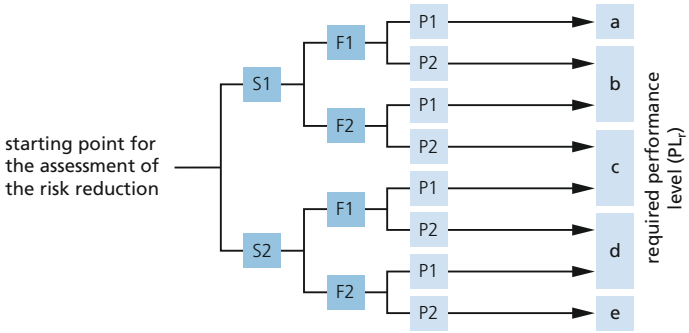


ifm sensors for industrial applications

Frequency and / or exposure to a hazard F		Probability of hazardous event W		Probability of avoidance P	
≤ 1 h	5	very high	5		
> 1 h to ≤ 1 day	5	likely	4		
> 1 day to ≤ 2 wks	4	possible	3	impossible	5
> 2 wks to ≤ 1 year	3	rarely	2	possible	3
> 1 year	2	negligible	1	likely	1

Class C = C + W + P				
3-4	5-7	8-10	11-13	14-15
SIL2	SIL2	SIL2	SIL3	SIL3
		SIL1	SIL2	SIL3
other measures			SIL1	SIL2
				SIL1

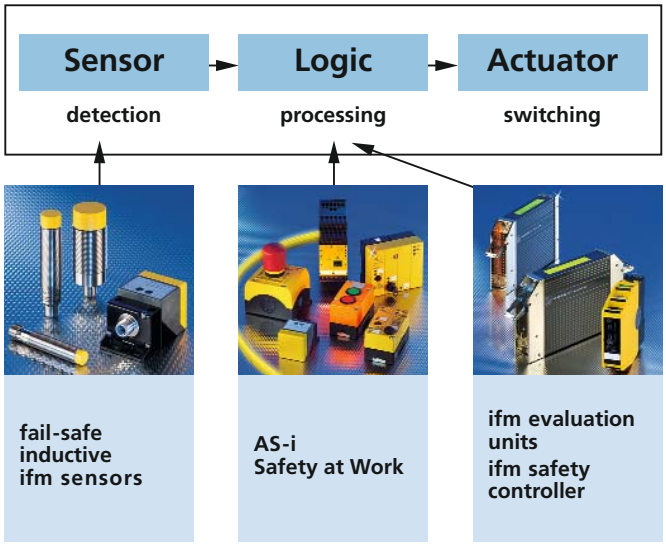
EN ISO 13849-1



Step 5
Determination of the achieved performance level, selection of the subsystems

The PL or $SIL_{(cl)}$ shall be estimated for each selected SRP/CS and SRECS and / or combination of SRP/CS and SRECS that perform a safety function.

SRECS or SRP/CS



fail-safe inductive ifm sensors

AS-i Safety at Work

ifm evaluation units ifm safety controller

Step 6
Validation / verification

Verification if the selected units or systems meet the requirements defined in the system design.

visit our website:

www.ifm.com

Overview ifm main catalogues:

Position sensors and object recognition
- Inductive sensors
- Capacitive sensors
- Magnetic sensors, cylinder sensors
- Safety technology
- Valve sensors
- Photoelectric sensors
- Object recognition
- Encoders
- Evaluation systems, power supplies
- Connection technology

Fluid sensors and diagnostic systems
- Level sensors
- Flow sensors
- Pressure sensors
- Temperature sensors
- Diagnostic systems
- Evaluation systems, power supplies
- Connection technology

Bus systems
- Bus system AS-Interface
- Power supplies
- Connection technology

Identification systems
- Multicode reading systems
- RF-identification systems
- Power supplies
- Connection technology

Control systems
- Control systems for mobile vehicles
- Connection technology

ifm electronic – close to you!

Over 70 locations worldwide – at a glance at **www.ifm.com**

ifm electronic gmbh
Teichstraße 4
45127 Essen
Tel. +49 / 0201 / 2 42 20
Fax +49 / 0201 / 2 42 22 00
E-Mail: info@ifm.com

ifm article no. 7511314 · We reserve the right to make technical alterations without prior notice. · Printed in Germany on non-chlorine bleached paper. 11/08